REMARKS

In view of the following remarks, reconsideration is respectfully requested.

I. 35 U.S.C. § 103 Rejections

Claims 1, 5-7, 12, 31, 36, 39, 43, 46 and 47 were rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Ahlstrom (U.S. 2003/0081747) and Abraham (U.S. 4,799,061). In addition, claims 8-11, 13-15, 30, 35, 38, 42 and 45 were rejected under 35 U.S.C. §103(a) as being unpatentable over Ahlstrom and Abraham in view of various combinations of Hill (U.S. 6,431,453), Kinugasa (U.S. 5,898,165), Yasuda (U.S. 4,703,347), Yasukura (U.S. 6,990,588), Lewis (U.S. 5,761,306) and Gobburu (U.S. 2002/0060246). These rejections are respectfully traversed for the following reasons.

Independent claim 1 recites an authentication system including an IC card of a forwarding agent, an authentication apparatus verifying authenticity of a visit by the forwarding agent, and a card reader for reading the IC card. In addition, claim 1 recites that (1) the IC card stores a first key that is obtained by executing a one-way function on a key that is identical to a secret key stored by the authentication apparatus, and (2) the authentication apparatus generates and outputs challenge data to the IC card via the card reader. Moreover, claim 1 recites that (3) the IC card receives the challenge data from the authentication apparatus, generates (and outputs to the authentication apparatus via the card reader) encrypted response data by encrypting the challenge data using the first key. Claim 1 also recites that (4) the authentication apparatus receives the encrypted response data from the IC card, generates a second key by executing a function, which is identical to the one-way function, on the secret key, generates decrypted data by decrypting the encrypted response data using the generated second key, and performs the authentication (of the visit of the forwarding agent) by judging whether or not the generated decrypted data matches the challenge data.

Regarding the above-mentioned one-way function, as recited in claim 1, the Applicants note that, for example, a one-way function is a function by which an output value Y (=f(X)) can be calculated from an input value X, but the input value X cannot be calculated from the output value Y. Therefore, according to the structure required by claim 1 and in terms of the one-way function Y (=f(X)), the secret key targeted for encryption is the input value (X) of the one way function, and the first key is the output value (Y) of the one way function, such that the first key (output value Y) is generated applying the one-way function f to the secret key.

With the above-described structure, even if the first key (output value Y) stored on the IC card is exposed, it is impossible to generate the secret key (input value X) from the first key (output value Y), due to the nature of the one-way function. As a result, the secret key will not be exposed, even if the first key stored on the IC card is obtained.

Initially, please note that the above-described 35 U.S.C. § 103(a) rejection relies on Ahlstrom and Abraham for teaching the above-mentioned distinguishing features (1)-(4), as recited in claim 1.

However, Ahlstrom merely teaches managing a person's entry/exit by using cards and card readers. Specifically, Ahlstrom teaches a system having two card readers (i.e., an inside card reader 114 and an outside card reader 112), such that both card readers are in communication with a main unit 116 (see Fig. 1; and paragraphs [0022], [0028] and [0031]). Additionally, Ahlstrom teaches that in order for the communication between the card readers and the main unit to be performed, an interrogation signal is used.

Thus, in view of the above, even though Ahlstrom teaches the use of an interrogation signal between the main unit and the card readers, it is clear that Ahlstrom does not teach that there is any encryption of the interrogation signal.

As a result, because Ahlstrom does not teach encrypting the interrogation signal, it is clear that Ahlstrom fails to disclose or suggest encrypting data using the first key that is obtained by executing a one-way function on a key that is identical with the secret key, as recited in claim 1.

Now turning to Abraham, the Applicants note that Abraham was relied upon for teaching the use of the "one-way function," as recited in claim 1. However, Abraham merely teaches the following four operations.

In **operation 1** a terminal 20 generates a value X ($=e_{k1}(RN)$) by encrypting a random number RN using key K1 and a secret key encryption method. In this case, the input value is RN and the output value is X (see Fig. 2; and col. 3).

In **operation 2** a card 10 generates a value Y ($=e_{k2}^{-1}(X)$) by decrypting a value X using a secret key K2. In this operation, the output value Y is generated using the output value X generated in **operation 1** (see Fig. 2; and col. 3). Specifically, the encrypted random number RN from **operation 1** (i.e., X) is decrypted using the secret key K2, such that if the secret keys K1 and K2 are equal, the random number RN can be obtained due to the nature of the secret key encryption method.

In **operation 3** the card 10 generates a value Z ($=e_Y(K2)$) by encrypting the secret key K2 using the decrypted value Y generated in **operation 2**. In this operation, the input value is the secret key K2 and the output value is Z (see Fig. 2; and col. 3).

In **operation 4** the terminal 20 generates a value A ($=e_{RN}^{-1}(Z)$) by decrypting the value Z using the random number RN. In this operation, the output value A is generated using the output value Z generated in **operation 3** (see Fig. 2; and col. 3). Specifically, the encrypted secret key K2 generated in **operation 3** is decrypted using the random number RN, such that if the secret keys K1 and K2 are equal, the random number RN should be used in operation 3, and by the decryption performed in operation 4, the secret key K2 can be obtained due to the nature of the secret key encryption method.

Therefore, according to Abraham, when both the terminal 20 and the card 10 have the same secret key, the result of the judgment of the block 39 goes to line 40, as shown in Fig. 2, and the card 10 is authenticated successfully. However, when this occurs, the secret key K2 could be obtained.

Furthermore, the Applicants note that the Office Action equates the claimed one-way function with the function for decrypting the value Z using the secret key to obtain value A in the secret key encryption, as disclosed by Abraham. However, the Applicants respectfully submit that the function for decrypting the value Z, as disclosed by Abraham, cannot be a one-way function for the following reasons.

Initially, assume that the function for decrypting the value Z using the secret key to obtain value A is a one-way function. Accordingly, based on the structure of the one-way function, when the secret keys K1 and K2 are equal, the random number RN should not be obtainable in operation 2 and the secret keys K2 and K1 should not be obtainable in operation 4.

Accordingly, assuming that the function for decrypting Z is a one-way function, when the secret keys K1 and K2 are equal, the card 10 will be judged as not being authentic, when actually, according to Abraham, the card 10 should be judged as being authentic. Therefore, the one-way function cannot be used for decrypting the value Z using the secret key to obtain value A.

Thus, for the reasons discussed above, Abraham cannot be said to disclose or suggest the encryption using the one-way function, as required by claim 1.

Furthermore, as a result of Abraham not disclosing or suggesting the one-way function, Abraham clearly teaches that <u>when the key K2 stored in the card 10 is exposed, the key K1 stored in the terminal 20 is also exposed</u>. Accordingly, Abraham cannot be said to disclose or suggest above-mentioned distinguishing features (1)-(4) as required by claim 1.

Put another way, in view of the above, it is clear that Abraham teaches encrypting using a two-way function, and fails to disclose or suggest that (i) the IC card receives the challenge data from the authentication apparatus, generates (and outputs to the authentication apparatus) encrypted response data by encrypting the challenge data using the first key, and (ii) the authentication apparatus receives the encrypted response data from the IC card, <u>generates a second key by executing a function, which is identical to the one-way function, on the secret key</u>, generates decrypted data by decrypting the encrypted response data using the generated second key, and performs the authentication of the visit of the forwarding agent by judging whether or not the generated decrypted data matches the challenge data, as recited in claim 1.

Therefore, because of the above-mentioned distinctions it is believed clear that claim 1 and claims 5-15 and 30 that depend therefrom would not have been obvious or result from any combination of Ahlstrom and Abraham.

In light of the discussion above, the combination of Ahlstrom and Abraham <u>does not</u> provide the above-mentioned benefits of the structure required by claim 1, such that, even if the first key stored on the IC card is exposed, it is <u>impossible to generate the secret key (input value</u>

X) from the first key (output value Y), due to the nature of the one-way function. As a result, the secret key will not be exposed, even if the first key stored on the IC card is obtained.

On the other hand, the result of the combination of Ahlstrom and Abraham is that when the key K2 of the card is exposed, then the key K1 of the terminal is also exposed, and when the keys K1 and K2 are equal the random number RN can be obtained, which reduces the security level of the security system.

Furthermore, there is no disclosure or suggestion in Ahlstrom and/or Abraham or elsewhere in the prior art of record which would have caused a person of ordinary skill in the art to modify Ahlstrom and/or Abraham to obtain the invention of independent claim 1. Accordingly, it is respectfully submitted that independent claim 1 and claims 5-15 and 30 that depend therefrom are clearly allowable over the prior art of record.

Regarding dependent claims 8-11, 13-15 and 30, which were rejected under 35 U.S.C. §103(a) as being unpatentable over Ahlstrom and Abraham (main references) in view of various combinations of Hill, Kinugasa, Yasuda, Yasukura, Lewis and Gobburu (additional references), it is respectfully submitted that these additional references do not disclose or suggest the above-discussed features of independent claim 1 which are lacking from the main references. Therefore, no obvious combination of the main references with any of the additional references would result in, or otherwise render obvious, the invention recited independent claim 1 and claims 5-15 and 30 that depend therefrom.

Independent claims 31, 39, 46 and 47 are directed to an apparatus, a portable recording medium, a method and a program, respectively and each recite features that correspond to the above-mentioned distinguishing features of independent claim 1. Thus, for the same reasons discussed above, it is respectfully submitted that independent claims 31, 39, 46 and 47 and claims 35, 36, 38, 42, 43 and 45 that depend therefrom are allowable over the prior art of record.

II. Conclusion

In view of the above remarks, it is submitted that the present application is now in condition for allowance and an early notification thereof is earnestly requested. The Examiner is invited to contact the undersigned by telephone to resolve any remaining issues.

Respectfully submitted,

Masao NONAKA et al.
/Andrew L. Dunlap/
By 2010.10.07 08:39:39 -04'00'
Andrew L. Dunlap
Registration No. 60,554
Attorney for Applicants

ALD/led
Washington, D.C. 20005-1503
Telephone (202) 721-8200
Facsimile (202) 721-8250
October 7, 2010